

HERMITIAN CODES AND COMPLETE INTERSECTIONS

CHIARA MARCOLLA AND MARGHERITA ROGGERO

ABSTRACT. In this paper we present a geometrical characterization for the minimum-weight codewords of the Hermitian codes over the fields \mathbb{F}_{q^2} in the third and fourth phase, namely with distance $d \geq q^2 - q$.

We consider the unique writing $\mu q + \lambda(q + 1)$ of the distance d with μ, λ non negative integers, and $\mu \leq q$, and prove that the minimum-weight codewords correspond to complete intersection divisors cut on the Hermitian curve \mathcal{H} by curves \mathcal{X} of degree $\mu + \lambda$ having $x^\mu y^\lambda$ as leading term w.r.t. the **DegRevLex** term order (with $y > x$).

Moreover, we show that any such curve \mathcal{X} corresponds to minimum-weight codewords provided that the complete intersection divisor $\mathcal{H} \cap \mathcal{X}$ is made of simple \mathbb{F}_{q^2} -points.

1. INTRODUCTION

Let q be a power of a prime. The *Hermitian curve* \mathcal{H} is the affine, plane curve defined by the polynomial $x^{q+1} = y^q + y$. It is a smooth curve of genus $g = \frac{q^2 - q}{2}$ with only one point at infinity. The curve \mathcal{H} is the best known example of *maximal curve*, that is with the maximum number of \mathbb{F}_{q^2} -points allowed by the Hasse-Weil bound [16].

Starting from the Hermitian curve and any positive integer m , it is possible to construct the one-point Goppa codes C_m on \mathcal{H} , that is called *Hermitian codes*. This is by far the most studied among Goppa codes, due to the good properties of the Hermitian curve and the simple basis of its Riemann-Roch space [19], which can be written explicitly.

For a thorough exposition of the main features of Hermitian curves and codes we refer to [6] and to Section 8.3 of [19].

In 1988, Stichtenoth [18] introduces the Hermitian codes describing their generator and parity-check matrices. Moreover, for any $m > q^2 - q - 2$, he finds a formula for the distance d of C_m . A few years later, Yang and Kumar [20] bring to completion Stichtenoth work finding the distance of the remaining codes C_m . Moreover, Yang [21] and Munuera [13] obtain the values of many *generalized Hamming weights*

2010 *Mathematics Subject Classification.* 11G20, 11T71.

Key words and phrases. Hermitian code, minimum-weight codeword, complete intersection.

also called *weight hierarchies*. Finally, Barbero and Munera [2] find the complete sequence of weight hierarchies of Hermitian codes by an exhaustive computation of the bounds given by Heijnen and Pellikaan [5].

In [7] the Hermitian codes are seen as a sub-family of evaluation codes. Using this different approach, the authors divide the codes C_m in four *phases* with respect to the integer m , and for each of them give explicit formulas linking dimension and distance. In this paper we adopt their classification of Hermitian codes in four phases (with minor changes, as summarized in Table 1).

Afterwards, the research about Hermitian codes branches out in several different lines. Some papers, as for instance [8, 9, 11, 14], deal with the problem of finding efficient algorithms for the decoding of the Hermitian codes.

An hard problem is that of determining the weight distribution, in particular the small-weight distribution. So far, few partial results are known, and the first of them appears only in 2011 ([15]).

The geometric characterization of the small-weight codewords of the Hermitian code C_m for a few cases of m (mainly in the first and second phase) can be found in [1, 3, 4, 12, 15]. In particular in [15] and [12], the first author of this paper and her co-authors study Hermitian codes C_m with distance $d \leq q$, that is with $m \leq q^2 - 2$ (first phase). They prove that the points corresponding to any minimum-weight codeword of C_m lie in the intersection between a line and \mathcal{H} ; on the other hand, any set of d points in such a *complete intersection* corresponds to minimum-weight codewords. This characterization allows the authors to compute the number of minimum-weight codewords.

In 2012, Couvreur [3] investigate the minimum-weight codewords problem for codes over an affine-variety \mathcal{X} by a new method. Quoting Couvreur paper *the approach is based on problems á la Cayley-Bacharach and consists in describing the minimal configurations of points on \mathcal{X} which fail to impose independent conditions on forms of some degree*.

As an application of this approach, in [4] the authors find a geometric characterization of small-weight codewords of C_m for some m and $d \leq 3q - 6$ (first and second phase). In particular they prove that the set of points corresponding to a minimum-weight codeword (or a subset of them) is a cut on \mathcal{H} by either a line, or a conic, or the complete intersection of two curves of degrees $q - 2$ and 3. A similar result is found for all codewords of the first phase having weight $v \leq 2d - 3$.

A new proof of the above results and some new information about the small-weight codewords of Hermitian codes C_m with $m \leq q^2 + q$ and $d = 2q + 2, 2q + 1, 2q$ or $d \leq q$ are presented in [1].

In this paper we provide a geometric characterization for minimum weight codewords of any Hermitian code C_m with $m \geq 2q^2 - 2q - 2$. Our main result is the following theorem.

Theorem (Theorem 4.1). *Let C_m be an Hermitian Code with $m \geq 2q^2 - 2q - 2$ and distance $d = m - q^2 + q - 2$. Let λ, μ be the non-negative integers such that $d = \mu q + \lambda(q + 1)$ and $\mu \leq q$ and let D be a divisor on the Hermitian curve \mathcal{H} made of simple points with coordinates in \mathbb{F}_{q^2} .*

Then D corresponds to a minimum-weight codeword if and only if it is the complete intersection of \mathcal{H} and a curve \mathcal{X} of degree $\mu + \lambda$ defined by a polynomial F whose leading term w.r.t. the term order DegRevLex (with $y > x$) is $x^\mu y^\lambda$.

A generalization of this result to codes of the other phases and to codewords of small weight is in progress. We are confident that, from this strong geometric characterization, also the explicit computation of the weight distribution will follow.

The paper is organized as follows:

- In Section 2 we recall some basic definitions and we introduce the term ordering that is the keystone of our new approach. Moreover, we prove some preliminary results about Hermitian codes and complete intersection divisors on the Hermitian curve \mathcal{H} .
- In Section 3 we study the Hermitian codes C_m with $m \geq 2q^2 - 2q - 2$. The main result of this section is Theorem 3.3 which will be key tools in the final section. In some sense it generalizes the classical results by Stichtenoth [18] about the distance formula. Indeed, in Corollary 3.4 we recover this same formula as a special case of what is proved in Theorem 3.3.
- In Section 4 we state and prove Theorem 4.1, which gives a geometric characterization for any minimum-weight codewords of the Hermitian codes C_m with $m \geq 2q^2 - 2q - 2$.
- At the end we draw the conclusions.

2. GENERALITIES AND PRELIMINARY RESULTS

2.1. The Hermitian curve. Let \mathbb{F}_{q^2} be the finite field with q^2 elements, where q is a power of a prime and let K be its algebraic closure. For any ideal I in the polynomial ring $\mathbb{F}_{q^2}[x, y]$ we denote by $\mathcal{V}(I)$ the corresponding variety in \mathbb{A}_K^2 ; if $g_1, \dots, g_s \in \mathbb{F}_{q^2}[x, y]$, we denote by (g_1, \dots, g_s) the ideal they generate.

The *Hermitian curve* \mathcal{H} is the curve in the affine plane \mathbb{A}_K defined by the polynomial $H := x^{q+1} - y^q - y$. We will denote by $I_{\mathcal{H}}$ the ideal in $\mathbb{F}_{q^2}[x, y]$ generated by H and by $A_{\mathcal{H}}$ the coordinate ring $\mathbb{F}_{q^2}[x, y]/I_{\mathcal{H}}$ of \mathcal{H} .

The curve \mathcal{H} has genus $g = \frac{q(q-1)}{2}$ and $n := q^3$ closed points with coordinates in \mathbb{F}_{q^2} (\mathbb{F}_{q^2} -points for short), that we will always denote by P_1, \dots, P_n . The projective closure $\overline{\mathcal{H}}$ of \mathcal{H} in \mathbb{P}_K^2 contains only one more point $P_\infty = [0 : 0 : 1]$, so that $\overline{\mathcal{H}}$ has $q^3 + 1$ \mathbb{F}_{q^2} -points [16].

In the following, we will denote by E the zero-dimensional scheme of degree n composed by all the \mathbb{F}_{q^2} -points of \mathcal{H} .

Definition 2.1. An \mathbb{F}_{q^2} -divisor over the Hermitian curve is a divisor $D = \sum_{i=1}^{\delta} Q_i$ where the Q_i 's are pairwise distinct \mathbb{F}_{q^2} -points of \mathcal{H} . We will denote by $|D|$ the degree δ of D . We can also write $D = \{Q_1, \dots, Q_\delta\}$; in particular, $E = \{P_1, \dots, P_n\}$ and D is a \mathbb{F}_{q^2} -divisor on \mathcal{H} if and only if $D \subseteq E$.

We denote by I_D the ideal generated by all polynomials in $\mathbb{F}_{q^2}[x, y]$ vanishing on D and by A_D the quotient ring $\mathbb{F}_{q^2}[x, y]/I_D$.

Lemma 2.2. *In the above notations, we have $A_E = \mathbb{F}_{q^2}[x, y]/\langle H, x^{q^2} - x, y^{q^2} - y \rangle$. Moreover, if D is a \mathbb{F}_{q^2} -divisor on \mathcal{H} , then A_D is a quotient of A_E .*

Proof. Since by definition E is a reduced sub-scheme of \mathcal{H} and its points are \mathbb{F}_{q^2} -rational, then $I_E \supseteq \langle H, x^{q^2} - x, y^{q^2} - y \rangle$. Vice versa $\langle H, x^{q^2} - x, y^{q^2} - y \rangle$ define a zero-dimensional scheme of degree q^3 . So $I_E = \langle H, x^{q^2} - x, y^{q^2} - y \rangle$.

For the second fact it is sufficient to recall that D is a \mathbb{F}_{q^2} -divisor of \mathcal{H} if and only if $D \subseteq E$, hence $I_D \supseteq I_E$. \square

2.2. A quick sketch on the affine-variety codes. Let C be a linear code over \mathbb{F}_{q^2} .

We recall that a *dual code* C^\perp of C is formed by all vectors \mathbf{v} such that $G\mathbf{v}^T = 0$ and a generator matrix of C^\perp is called a *parity-check matrix* of the code C . Moreover if $\mathbf{c} = (c_1, \dots, c_n) \in C$ is a codeword, then the *weight* of \mathbf{c} is the number of c_i that are different from 0, whereas, its *support* $\text{Supp}(\mathbf{c})$ is the set of indices corresponding to the non-zero entries. In our case, the entries of a codeword \mathbf{c} are labeled by the \mathbb{F}_{q^2} -points of the Hermitian curve and we will identify its support with the \mathbb{F}_{q^2} -divisor D which is the sum of points that correspond to the non-zero entries. Finally, the *distance* of a code is the minimum weight of its non-zero codewords.

We now briefly recall the definition of affine-variety codes of which the Hermitian codes are special cases.

Let us consider an ideal $I \subset \mathbb{F}_{q^2}[x, y]$ such that $\{x^{q^2} - x, y^{q^2} - y\} \subset I$. Then I is zero-dimensional and radical [17]. If $\mathcal{V}(I) = \{Q_1, \dots, Q_r\}$, then the *evaluation map*

ϕ_I is defined in the following way:

$$(2.1) \quad \begin{array}{ccc} \phi_I : R = \mathbb{F}_{q^2}[x, y]/I & \longrightarrow & (\mathbb{F}_{q^2})^r \\ f & \longmapsto & (f(Q_1), \dots, f(Q_r)). \end{array}$$

Definition 2.3. Let $L \subseteq R$ be an \mathbb{F}_{q^2} -vector subspace of R . The **affine-variety code** $C(I, L)$ is the image $\phi_I(L)$ and the affine-variety code $C(I, L)^\perp$ is its dual code.

We fix an order for the points Q_1, \dots, Q_r and a basis f_1, \dots, f_s of L . Then $C(I, L)$ is given by the matrix G , called *generator matrix* of the code, having in the (i, j) -position the evaluation of f_i in the point Q_j .

In this paper, the Hermitian codes are seen as dual codes of special subspace. We associate to the Hermitian curve \mathcal{H} defined by $H = x^{q+1} - y^q - y$ the weight vector $w := [w(x) = q, w(y) = q + 1]$, so any monomial $x^r y^s$ has weight-degree $w(x^r y^s) = rq + s(q + 1)$. For any fixed positive integer m , we denote by V_m the subspace of A_E generated by (the classes of) the monomials of weight degree less or equal than m . We denote by C_m the corresponding Hermitian code (that is a dual code). Note that, usually, the set of monomials having weight degree $\leq m$ are not linearly independent. For this reason, we select a suitable set of monomials \mathcal{B} (a basis for A_E) such that, for every m , $\mathcal{B} \cap V_m$ is a basis for V_m . In this way the parity-check matrix of any code C_m has exactly $n - k$ rows where k is the dimension of the code. To choose this basis is convenient to use a term order.

2.3. Term ordering and Hermitian codes. Depending on which term ordering \prec we choose, the initial ideal $\text{In}_\prec(I_E)$ of I_E can be either $J_1 = \langle y^q, x^{q^2} \rangle$ or $J_2 = \langle x^{q+1}, xy^{q^2-q}, y^{q^2} \rangle$. In both cases the first monomial is the leading monomial of H , the other ones derive by the field equations. Therefore, we have only two different bases for A_E given by the set of monomials of $\mathcal{N}(\text{In}_\prec(I_E))$, which are:

$$(2.2) \quad \mathcal{B}_{J_1} = \{x^r y^s \mid r \leq q^2 - 1, s \leq q - 1\}$$

$$(2.3) \quad \mathcal{B}_{J_2} = \{x^r y^s \mid 1 \leq r \leq q, s \leq q^2 - q - 1\} \cup \{y^s \mid q^2 - q \leq s \leq q^2 - 1\}$$

The term order we usually find in literature is the weighed term $<_w$ associated to the weight vector $w = [q, q + 1]$ (and **Lex** with $y > x$ as a “tie-breaker”). More precisely:

$$x^r y^s <_w x^{r'} y^{s'} \iff \begin{cases} rq + s(q + 1) < r'q + s'(q + 1) & \text{or} \\ rq + s(q + 1) = r'q + s'(q + 1) \text{ and } s < s' \end{cases}$$

Choosing this term order, we obtain $\text{In}(I_{\mathcal{H}}) = \langle y^q \rangle$ and $\text{In}(I_E) = \langle y^q, x^{q^2} \rangle = J_1$. Then, the usual monomial basis is that given in (2.2).

However, in this paper we prefer to use the term order **DegRevLex** with $y > x$, denoted in the following by \prec . It gives $\text{In}_{\prec}(I_{\mathcal{H}}) = \langle x^{q+1} \rangle$ and $\text{In}_{\prec}(I_E) = \langle x^{q+1}, xy^{q^2-q}, y^{q^2} \rangle$. Then, we will always consider as a basis of A_E that given in (2.3), in the following simply denoted by \mathcal{B} .

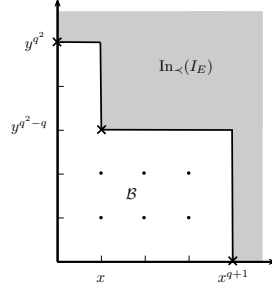


FIGURE 1. The set of monomials in \mathcal{B}

Remark 2.4. If F is a polynomial in $\mathbb{F}_{q^2}[x, y]$ such that $\partial_x(F) \leq q$, then $\text{LM}_{\prec}(F) = \text{LM}_{<_w}(F)$. In other words, the ordering by \prec on the set of monomials \mathcal{B} is equal to the one given by $<_w$. As a consequence, the w -degrees of the monomials in \mathcal{B} are pairwise different; they all are integer numbers between 0 and $q^3 + (q^2 - q) - 1 = n + 2g - 1$, but a few of these integers are missing. Indeed, if g is the genus of the hermitian curve, there are g numbers between 1 and $2g - 1$ that cannot be obtained as the w -degree of a monomial: they are the gaps of the semigroup generated by q and $q + 1$. Moreover, we cannot find among the w -degrees of monomials in \mathcal{B} a set of g numbers larger than $n - 1$: though there are monomials having those w -degrees, they do not belong to \mathcal{B} , since they are multiple of $xy^{q^2-q} \in \text{In}_{\prec}(I_E)$.

Summarizing the construction, an *Hermitian code* is defined in the following way. Let us fix any order P_1, \dots, P_n of the n points of the set E of \mathbb{F}_{q^2} -points of the Hermitian curve \mathcal{H} .

Definition 2.5. Let \mathcal{B} be as (2.3), m be any integer $\leq n + 2g - 2$, V_m be the vector space in $\subseteq A_E$ generated by all the monomials of w -degree less than or equal to m , and

$$\mathcal{B}_m = \mathcal{B} \cap V_m = \{x^r y^s \in \mathcal{B} \mid rq + s(q + 1) \leq m\}$$

its basis. Then the **Hermitian code** C_m is the \mathbb{F}_{q^2} -vector space $(\text{Span}_{\mathbb{F}_{q^2}} \langle \phi_{I_E}(\mathcal{B}_m) \rangle)^\perp$ where ϕ_{I_E} is the evaluation map (2.1) at the points of E .

The Hermitian codes can be divided in four phases [7], any of them having specific explicit formulas linking their dimension and their distance [10], as in Table 1.

TABLE 1. The four “phases” of Hermitian codes [10].

Phase	m	Distance d	Dimension k
1	$0 \leq m \leq q^2 - 2$ $m = aq + b$ $0 \leq b \leq a \leq q - 1$ $b \neq q - 1$	$\begin{matrix} a+1 & a > b \\ a+2 & a = b \end{matrix} \iff d \leq q$	$q^3 - \frac{a(a+1)}{2} - (b+1)$
2	$q^2 - 1 \leq m \leq 4g - 3$ $m = 2q^2 - q - aq - b - 3$ $1 \leq a \leq q - 2$ $0 \leq b \leq q - 2$	$\begin{matrix} (q-a)q - b - 1 & a \leq b \\ (q-a)q & a > b \end{matrix}$	$n - g - q^2 + aq + b + 2$
3	$4g - 2 \leq m \leq n - 2$	$m - 2g + 2$	$n - m + g - 1$
4	$n - 1 \leq m \leq n + 2g - 2$ $m = n + 2g - 2 - aq - b$ $0 \leq b \leq a \leq q - 2,$	$n - aq - b$	$\frac{a(a+1)}{2} + b + 1$

2.4. Hermitian codes C_m with $m \geq q^2 - 1$. In the following we can associate to any Hermitian code C_m the uniquely defined pair of non negative integers (μ, β) such that $m = \mu q + \beta(q + 1)$ and $\mu \leq q$ (Remark 2.4). As we are considering only the case $m \geq q^2 - 1$, these integers do exist.

It is a straightforward consequence of Definition 2.5 that $C_m \supseteq C_{m+1}$ for every m . If in \mathcal{B} there is no monomial of w -degree $m + 1$, then $V_m = V_{m+1}$, hence $C_m = C_{m+1}$. For this reason, without loosing in generality in the following **we only consider codes C_m such that \mathcal{B} contains a monomial of w -degree $m + 1$.**

On the other hand, for values of m in the range corresponding the forth phase, the maximum w -degree of the monomials in \mathcal{B}_m can be less than m .

Example 2.6. Let us consider the case $q = 3$. The first possible value after the third phase is 26. However, we do not label the code corresponding to V_{26} as C_{26} , but as C_{27} . Indeed, $V_{26} = V_{27}$, since the monomial $x^r y^s$ with $r \leq 3$ and w -degree $26 + 1$, that is xy^6 , is a generator of $\text{In}_\prec(I_E) = \langle x^4, xy^6, y^9 \rangle$ and it is not an element of \mathcal{B} , but we can find in \mathcal{B} the monomial y^7 whose w -degree is $27 + 1$, hence $V_{27} \neq V_{28}$.

Note that for every monomial $x^r y^s$ of \mathcal{B} we have

$$x^r y^s \in \mathcal{B} \setminus \mathcal{B}_m \iff \text{either } r + s > \mu + \beta \text{ or } r + s = \mu + \beta \text{ and } r < \mu.$$

In the following, for any \mathbb{F}_{q^2} -divisor D over the Hermitian curve we will denote by $V_{m,D}$ the image of V_m in A_D . We observe that D contains the support of some codeword of C_m if $V_{m,D}$ has dimension less than $|D|$. We can summarize all these facts in the following:

Proposition 2.7. *Let $1 \leq v \leq n$. Let J_v be the ideal in $\mathbb{F}_q[x_1, \dots, x_v, y_1, \dots, y_v, z_1, \dots, z_v]$ generated by*

$$(2.4) \quad \sum_{i=1}^v z_i x_i^r y_i^s = 0 \quad \text{for} \quad x^r y^s \in \mathcal{B}_m$$

$$(2.5) \quad x_i^{q+1} - y_i^q - y_i = 0 \quad \text{for} \quad i = 1, \dots, v$$

$$(2.6) \quad x_i^{q^2} - x_i = 0 \quad y_i^{q^2} - y_i = 0 \quad z_i^{q^2-1} - 1 = 0 \quad \text{for} \quad i = 1, \dots, v$$

$$(2.7) \quad ((x_i - x_j)^{q^2-1} - 1)((y_i - y_j)^{q^2-1} - 1) = 0 \quad \text{for} \quad 1 \leq i < j \leq v.$$

Then any solution of J_v corresponds to a codeword of C_m with weight v .

Proof. See Proposition 1 of [12]. □

The following proposition is a crucial tool in our arguments.

Proposition 2.8. *Let D be a \mathbb{F}_{q^2} -divisor over Hermitian curve. Then the following are equivalent for the Hermitian code C_m with $m = \mu q + \beta(q+1)$:*

- (i) $\exists \mathbf{c} \in C_m$ with $\mathbf{c} \neq 0$ such that $\text{Supp}(\mathbf{c}) \subseteq D$
- (ii) $V_{m,D}$ has dimension less than $|D|$ as vector space over \mathbb{F}_{q^2} .
- (iii) There exists a monomial $x^a y^b \in \mathcal{N}(\text{In}_{\prec}(I_D))$ such that $m+1 \leq w(x^a y^b) \leq m+q+1$.
- (iv) If $\mu > 0$, $\mathcal{N}(\text{In}_{\prec}(I_D))$ contains at least one monomial in

$$(2.8) \quad \mathcal{L}_1 := \{x^{\mu-i} y^{\beta+i} \text{ with } 1 \leq i \leq \mu\} \cup \{x^{q-j} y^{\beta+\mu-q+j+1} \text{ with } 0 \leq j \leq q-\mu\};$$

otherwise, $\mu = 0$ and $\mathcal{N}(\text{In}_{\prec}(I_D))$ contains at least one monomial in

$$(2.9) \quad \mathcal{L}_2 := \{x^{q-j} y^{\beta-q+j+1}, \text{ with } 0 \leq j \leq q\}.$$

Proof. Let H_E and $H_{E,m}$ be the parity-check matrices respectively of the trivial code and of C_m and consider their sub-matrices M_D and $M_{D,m}$ obtained only considering the columns corresponding to the points $P_i \in D$. More explicitly, if $\delta = |D|$ and $D = \{P_{i_1}, \dots, P_{i_\delta}\}$ their j -th column is formed by the evaluation of monomials of \mathcal{B} and, respectively, \mathcal{B}_m at P_{i_j} . The codewords of weight v of C_m are the solutions of the system J_v of Proposition 2.7, and in particular they satisfy the equation (2.4), that is, they are solutions of the linear system $H_{E,m} \cdot Z^T = 0$, where $Z = (z_1, \dots, z_n)$. The list of non-zero components of any codeword $\mathbf{c} \in C_m$ with $\text{Supp}(\mathbf{c}) \subseteq D$ are given by a solution of the linear system $M_{D,m} \cdot Z_D^T = 0$, where $Z_D = (z_{i_1}, \dots, z_{i_\delta})$. Therefore, there exist non-zero codewords $\mathbf{c} \in C_m$ such that $\text{Supp}(\mathbf{c}) \subseteq D$ if and only if $\text{rk}(M_{D,m}) < |D|$, that is, (ii) is verified.

By Lemma 2.2 the basis of A_D given by the monomials of $\mathcal{N}(\text{In}_{\prec}(I_D))$ is a subset of \mathcal{B} . Since $\text{rk}(M_D) = |D|$, then (i) is verified if and only if there exists a monomial $x^r y^s \in \mathcal{B} \setminus \mathcal{B}_m$ that belongs to $\mathcal{N}(\text{In}_{\prec}(I_D))$.

Finally we prove that there is a similar monomial whose w -degree is less than or equal to $m + q + 2$. If this is not true for $x^r y^s$, then $\mathcal{N}(\text{In}_{\prec}(I_D))$ also contains either $x^{r-1} y^s$ or $x^r y^{s-1}$. Note that these two monomials have w -degree still larger than m . We can repeat this argument until we get a monomial with a sufficiently low w -degree.

The equivalence between (iii) and (iv) is obvious, being (iv) a more explicit rewriting of (iii). \square

2.5. Complete intersections on \mathcal{H} . In this section we use the Bézout Theorem to find some properties of the zero-dimensional schemes that are complete intersection of \mathcal{H} with another curve \mathcal{X} . To this purpose, we must also consider the possible intersections at infinity. We recall that the projective closure $\overline{\mathcal{H}}$ of \mathcal{H} has a single point at infinity $P_\infty = [x_0 = 0 : x_1 = 0 : x_2]$ where $x_1/x_0 = x$ and $x_2/x_0 = y$. It is a smooth, inflexion point with tangent line $x_0 = 0$.

Proposition 2.9. *Let $F \in \mathbb{F}_{q^2}[x, y]$ be a polynomial such that $\partial_x(F) \leq q$ and let \mathcal{X} be the curve given by $F = 0$. If $\text{LM}_{\prec}(F) = x^r y^s$, then*

- (i) $\text{In}_{\prec}(\langle H, F \rangle) = \langle x^{q+1}, x^r y^s, y^{s+q} \rangle$ when $s > 0$ and
- (ii) $\text{In}_{\prec}(\langle H, F \rangle) = \langle x^r, y^q \rangle$ when $s = 0$.

Moreover, the degree of the divisor D cut on \mathcal{H} by \mathcal{X} is $rq + s(q + 1)$.

Proof. We first prove that $|D| = rq + s(q + 1)$. Since the term order \prec is degree-compatible, the degree of F is equal to the degree $r + s$ of its leading term. By Bézout Theorem, the degree of the divisor \overline{D} cut on $\overline{\mathcal{H}}$ by the projective closure $\overline{\mathcal{X}}$ of \mathcal{X} is $(r + s)(q + 1)$. It remains to prove that the intersection multiplicity of the two curves at P_∞ is r .

We chose the affine chart of \mathbb{P}^2 around P_∞ given by $x_2 \neq 0$. To this aim we homogenize F and H , by setting $x = x_1/x_0$, $y = x_2/x_0$ and then de-homogenize by setting $x_2 = 1, x_0 = z, x_1 = x$. Let F' and H' be the polynomials obtained in this way. Obviously $H' = x^{q+1} - z^q - z$. For what concerns F' , we observe that all monomials of maximum degree in the support of F are divisible by x^r ; hence every monomial of F' is divisible by z and/or by x^r ; moreover x^r itself is in the support of F' .

Without modifying the intersection multiplicity at P_∞ , we can replace any occurrence of z in F' by $H' + z = x^{q+1} - z^q$, until we get a polynomial F'' having x^r as the only monomial of minimum degree. Therefore, $\text{mult}_{P_\infty}(\overline{\mathcal{H}}, \overline{\mathcal{X}}) = \text{mult}_{P_\infty}(H', F') = \text{mult}_{P_\infty}(H', F'') = r$, and we conclude $|D| = |\overline{D}| - |rP_\infty| = rq + s(q + 1)$.

Now we prove (i) and (ii). As the set of monomials $\mathcal{N}(\text{In}_{\prec}(I_D))$ is a basis for A_D , for what just proved we know that its cardinality is $rq + s(q + 1)$.

- (i) If $s > 0$, we can write F as $x^r y^s + x^{r+1} F_1 + F_2$ where $\partial F_1 = s - 1$ and $\partial F_2 < r + s$. We observe that the polynomial $x^{q+1-r} F - (y^s + x F_1) H$ is

an element of I_D and its leading monomial is y^{s+q} . Therefore, $\text{In}_{\prec}(I_D) \supseteq J := \langle x^{q+1}, x^r y^s, y^{s+q} \rangle$, so that $\mathcal{N}(\text{In}_{\prec}(I_D)) \subseteq \mathcal{N}(J)$. It is now easy to check that the cardinality of $\mathcal{N}(J)$ is exactly $rq + s(q+1)$ and get the equality $\text{In}_{\prec}(I_D) = J$.

- (ii) If $s = 0$ we can write F as $x^r + F_3$ where $\partial F_3 < r$. Again, we see that the polynomial $H - x^{q+1-r}F$ belongs to I_D and its leading monomial is y^q . Hence $\text{In}_{\prec}(I_D) \supseteq J' := \langle x^r, y^q \rangle$, so that $\mathcal{N}(\text{In}_{\prec}(I_D)) \subseteq \mathcal{N}(J')$. An easy computation shows that $|\mathcal{N}(J')| = rq$ and we conclude that $\text{In}_{\prec}(I_D) = J'$.

□

Corollary 2.10. *Let D be a divisor over \mathcal{H} and let $x^r y^s$ be a monomial in $\text{In}_{\prec}(I_D)$ with $r \leq q$. Then $|D| \leq rq + s(q+1)$.*

Proof. Let F be any polynomial in I_D such that $\text{LM}_{\prec}(F) = x^r y^s$. Then the degree of F is $r+s$ and the projective closure of the curve defined by F cuts on $\overline{\mathcal{H}}$ a divisor $D + D' + tP_{\infty}$ of degree $(r+s)(q+1)$. By Proposition 2.9 we know that $t = r$ and so $|D| \leq |D + D'| = (r+s)(q+1) - r = rq + s(q+1)$. □

3. MINIMUM DISTANCE OF HERMITIAN CODES OF THIRD AND FORTH PHASE

In this section we study the Hermitian codes C_m with $m \geq 2q^2 - 2q - 2$ and in particular, at the end of the section, we get a formula for their distance. What we obtain is nothing else than the well known formula first proved by Stichtenoth in [18]. However, we prefer to prove it directly since the preliminary results that will lead us to this proof, especially Theorem 3.3, are key tools in the final section.

Remark 3.1. We observe that in the new hypothesis, the numbers μ and β such that $m = \mu q + \beta(q+1)$ always satisfy the inequalities $0 \leq \mu \leq q$ and $\beta \geq q-2$. More generally if a, b are non-negative integers such that $a \leq q$ and $aq + b(q+1) \geq 2q^2 - 2q - 2$, then $b \geq q-2$.

Lemma 3.2. *Let D be a \mathbb{F}_{q^2} -divisor over \mathcal{H} which is the support of a non-zero codeword of C_m . Then I_D verifies at least one of the following conditions:*

- (i) *if $x^r \in \text{In}_{\prec}(I_D)$ and $x^{r-1} \notin \text{In}_{\prec}(I_D)$, then $r = q+1$;*
- (ii) *if $y^s \in \text{In}_{\prec}(I_D)$ and $y^{s-1} \notin \text{In}_{\prec}(I_D)$, then $s = q$.*

Proof. Since I_D is a zero-dimensional ideal, then $\text{In}_{\prec}(I_D)$ contains some power of x and of y : let x^r and y^s be the minimal ones. Obviously, $r \leq q+1$, as $H \in I_D$. We assume $r \leq q$, and prove that $s \leq q$.

Indeed, if F is any polynomial in I_D with leading monomial x^r , then we find in I_D also the polynomial $H - x^{q+1-r}F$ whose leading monomial is y^q .

It remains to prove that we cannot have both $r \leq q$ and $s \leq q-1$. In fact, if so,

$\text{In}_{\prec}(I_D) \supseteq \langle x^q, y^{q-1} \rangle$, that is $\mathcal{N}(\text{In}_{\prec}(I_D)) \subseteq \mathcal{N}(\langle x^q, y^{q-1} \rangle)$. The larger w -degree of monomials in $\mathcal{N}(\langle x^q, y^{q-1} \rangle)$ is $w(x^{q-1}y^{q-2}) = q^2 - 2q - 2 \leq m$, in contradiction with Proposition 2.8. \square

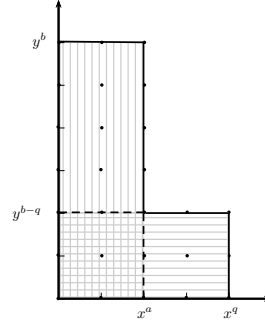
Theorem 3.3. *Let $x^ay^b \in \mathcal{B} \setminus \mathcal{B}_m$ such that $m+1 \leq w(x^ay^b) \leq m+q+1$.*

- (i) *If D is a \mathbb{F}_{q^2} -divisor over \mathcal{H} such that $x^ay^b \in \mathcal{N}(\text{In}_{\prec}(I_D))$ and which is the support of a codeword of C_m , then $|D| \geq w(x^ay^b) - (q^2 - q) + 1$.*
- (ii) *There exists a \mathbb{F}_{q^2} -divisor D' over \mathcal{H} corresponding to a codeword of C_m such that $x^ay^b \in \mathcal{N}(\text{In}_{\prec}(I_{D'}))$ and $|D'| = w(x^ay^b) - (q^2 - q) + 1$.*

Proof. By Remark 3.1 we have that $0 \leq a \leq q$ and $b \geq q-2$. We split the proof of the first item into three cases:

- If $b = q-2$, then $w(x^ay^b) \geq m+1$ if and only if $a = q$. Since $x^ay^b = x^qy^{q-2} \in \mathcal{N}(\text{In}_{\prec}(I_D))$, then $\mathcal{N}(\text{In}_{\prec}(I_D))$ also contains all $(q+1)(q-1)$ factors of x^qy^{q-2} . Therefore, $|D| = |\mathcal{N}(\text{In}_{\prec}(I_D))| \geq (q+1)(q-1) = w(x^ay^b) - (q^2 - q) + 1$.
- If $b = q-1$, we can argue as in the previous case: from $x^ay^{q-1} \in \mathcal{N}(\text{In}_{\prec}(I_D))$ we get $|D| = |\mathcal{N}(\text{In}_{\prec}(I_D))| \geq (a+1)q = w(x^ay^b) - (q^2 - q) + 1$.
- If $b \geq q$, then $y^q \notin \text{In}_{\prec}(I_D)$. As a consequence, we know by Lemma 3.2 that x^{q+1} is the minimal power of x in $\text{In}_{\prec}(I_D)$ and we deduce by Proposition 2.9 that $x^qy^{b-q} \notin \text{In}_{\prec}(I_D)$.

Computing the number of factors of the two monomials x^ay^b and x^qy^{b-q} we get $|D| = |\mathcal{N}(\text{In}_{\prec}(I_D))| \geq (a+1)(b+1) + (q+1)(b-q+1) - (a+1)(b-q+1) = w(x^ay^b) - (q^2 - q) + 1$.



Now we prove the second item, again splitting in cases. In all of them we can obtain D' as the divisor cut on \mathcal{H} by a curve \mathcal{Y} union of lines.

- If $a = q$ and $b \in \{q-2, q-1\}$, \mathcal{Y} is the union of $b+1$ horizontal lines passing through points of \mathcal{H} . In other words, the curve \mathcal{Y} is defined by a polynomial $F := \prod_{i=1}^{b+1} (y - k_i)$ such that $\text{Tr}(k_i) \neq 0$ for any i . So $\text{In}_{\prec}(I_{D'}) = \langle x^{q+1}, y^{b+1} \rangle$.
- If $a = b = q-1$, \mathcal{Y} is the union of q vertical lines passing through $q+1$ points of \mathcal{H} with non-zero x -coordinate, namely it is defined by a polynomial $F := \prod_{i=1}^q (x - k_i)$, with $k_i \neq 0$. So $\text{In}_{\prec}(I_{D'}) = \langle x^q, y^q \rangle$.
- If $b \geq q$, \mathcal{Y} is the union of $a+1$ vertical lines and $b+1-q$ non-vertical lines such that not two of them meet in a point of E . In other words, the

curve \mathcal{Y} is defined by a polynomial $F := \prod_{i=1}^{a+1} (x - \alpha_i) \prod_{j=1}^{b+1-q} (y - \beta_j)$ where $N(\alpha_i) \neq \text{Tr}(\beta_j)$ and $\text{Tr}(\beta_j) \neq 0$.

More precisely, if $a = 0$ we can set $F := x \cdot \prod_{j=1}^{b+1-q} (y - \beta_j)$ with $\text{Tr}(\beta_j) \neq 0$, whereas, if $a \geq 1$ it is sufficient to choose α_i, β_j such that $N(\alpha_i) = 1$, $\text{Tr}(\beta_j) \neq 0, 1$. In fact, if $a \geq 1$ then $b \leq q^2 - q - 1$ since $x^a y^b \in \mathcal{N}(\text{In}_{\prec}(I_E)) = \mathcal{N}(\text{In}_{\prec}(\langle x^{q+1}, xy^{q^2-q}, y^{q^2} \rangle))$. So we obtain at most $q + 1$ vertical lines and at most $(q - 2)q$ horizontal lines, that is, $a + 1 \leq q + 1$ and $b - q + 1 \leq (q - 2)q$. In this case, we have $\text{In}_{\prec}(I_{D'}) = \langle x^{q+1}, y^{b+1}, x^{a+1} y^{b+1-q} \rangle$.

□

We stress that the argument we use to prove the last part of the above theorem is directly inspired by the one used by Stichtenoth in [18] to explicitly exhibit some codewords of minimum weight.

Corollary 3.4. *Let C_m be an Hermitian code with $m \geq 2q^2 - 2q - 2$ such that $C_m \neq C_{m+1}$. Then the distance of C_m is $d = m - q^2 + q + 2 = m - 2g + 2$.*

Proof. By Proposition 2.8, if D is a \mathbb{F}_{q^2} -divisor over \mathcal{H} corresponding to a codeword of C_m , then $\mathcal{N}(\text{In}_{\prec}(I_D))$ contains a monomial $x^a y^b$ of $\mathcal{B} \setminus \mathcal{B}_m$. By Theorem 3.3, we have $|D| \geq w(x^a y^b) - q^2 + q + 1$, and there is a \mathbb{F}_{q^2} -divisor D' over \mathcal{H} for which we have equality. Therefore, the minimum w -degree of such divisors, namely the distance d of the code C_m , is that obtained when $x^a y^b$ is the monomial of w -degree in $\mathcal{B} \setminus \mathcal{B}_m$, that in our assumption is always $m + 1$. □

4. GEOMETRIC DESCRIPTION OF MINIMUM WEIGHT CODEWORDS

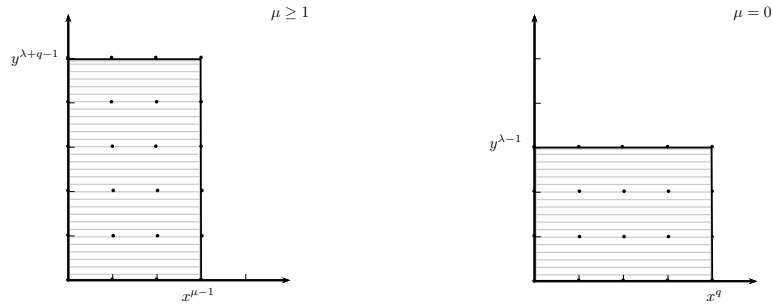
In this section we consider Hermitian codes C_m where m is an integer such that $2q^2 - 2q - 2 \leq m \leq n + 2g - 2$. Then, by Remark 3.1, we have that $m = \mu q + \beta(q + 1)$ with $0 \leq \mu \leq q$ and $\beta \geq q - 2$. Moreover, by Corollary 3.4, the distance of C_m is $d = \mu q + \lambda(q + 1)$ where $\lambda = \beta - q + 2$.

We recall that in \mathcal{B} there exists a monomial of w -degree $m + 1$.

Theorem 4.1. *Let C_m be the Hermitian code having distance $d = \mu q + \lambda(q + 1)$. Then:*

- (i) *Let D be a \mathbb{F}_{q^2} -divisor cut on \mathcal{H} by the curve defined by a polynomial F such that $\text{LM}_{\prec}(F) = x^{\mu} y^{\lambda}$. Then D corresponds to minimum weight codewords of C_m .*
- (ii) *Let D be a \mathbb{F}_{q^2} -divisor on \mathcal{H} corresponding to minimum weight codewords of C_m . Then there exists only one monomial in $\mathcal{N}(\text{In}_{\prec}(I_D))$ whose w -degree is larger than m , and its w -degree is exactly equal to $m + 1$. Moreover D is cut on \mathcal{H} by the curve defined by a polynomial F such that $\text{LM}_{\prec}(F) = x^{\mu} y^{\lambda}$.*

- Proof.* (i) By Proposition 2.9, if D is a \mathbb{F}_{q^2} -divisor cut on \mathcal{H} by the curve defined by a polynomial F such that $\text{LM}_{\prec}(F) = x^{\mu}y^{\lambda}$, then $|D| = \mu q + \lambda(q + 1)$. Moreover, if $\lambda \geq 1$, then $\text{LM}_{\prec}(\langle H, F \rangle) = \langle x^{q+1}, x^{\mu}y^{\lambda}, y^{\lambda+q} \rangle$; otherwise $\lambda = 0$ and $\text{In}_{\prec}(\langle H, F \rangle) = \langle x^{\mu}, y^q \rangle$. In both cases, $\mathcal{N}(\text{In}_{\prec}(I_D))$ contains a monomial of w -degree $m + 1$. By Lemma 2.8, D corresponds to codewords of weight $|D| = d$.
- (ii) By Theorem 3.3, in $\mathcal{N}(\text{In}_{\prec}(I_D))$ there is a monomial $x^a y^b$ with w -degree $m + 1$. It is easy to see that it is $x^{\mu-1}y^{\lambda+q-1}$ if $\mu \geq 1$, and $x^q y^{\lambda-1}$ if $\mu = 0$. Moreover we know that $|\mathcal{N}(\text{In}_{\prec}(I_D))| = d = m - (q^2 - q) + 2$ and that $\mathcal{N}(\text{In}_{\prec}(I_D))$ contains all the divisors of $x^a y^b$, whose number is $\mu(\lambda + q)$ if $\mu \geq 1$ and $(q + 1)\lambda$ if $\mu = 0$ (see Figure 2).

FIGURE 2. The sous-escalier of I_D .

We consider three different cases:

- Case $\mu = 0$. Since $d = \lambda(q + 1)$, the number of monomials dividing $x^a y^b$ are exactly as many as the monomials in $\mathcal{N}(\text{In}_{\prec}(I_D))$, hence $\mathcal{N}(\text{In}_{\prec}(I_D))$ is exactly the set of these monomials. Therefore, there exist a polynomial F in I_D such that $\text{LM}_{\prec}(F) = y^{\lambda}$. By Corollary 2.10 this polynomial cuts on \mathcal{H} a divisor D' which contains D and has the same degree of D , so $D' = D$.
- Case $\mu, \lambda > 0$. We observe that $x^q y^{\lambda-1}$ must belong to $\mathcal{N}(\text{In}_{\prec}(I_D))$. Otherwise, by Proposition 2.9, we would $y^{\lambda+q-1} \in \text{In}(I_D)$ and so also $x^{\mu-1}y^{\lambda+q-1} \in \text{In}_{\prec}(I_D)$, against what we have just proved. Computing the number of the divisors of $x^{\mu-1}y^{\lambda+q-1}$ and of $x^q y^{\lambda-1}$, we get exactly d (see Figure 3). Therefore, $\mathcal{N}(\text{In}_{\prec}(I_D))$ is formed by these monomials, since $|\mathcal{N}(\text{In}_{\prec}(I_D))| = d$. Moreover $x^{\mu}y^{\lambda}$, that does not divide neither $x^{\mu-1}y^{\lambda+q-1}$ nor $x^q y^{\lambda-1}$, belongs to $\text{In}_{\prec}(I_D)$. Then, there is a polynomial $F \in I_D$ with leading monomial $x^{\mu}y^{\lambda}$. By Corollary 2.10 the curve defined by F cuts D on \mathcal{H} .
- Case $\lambda = 0$. The monomial $x^a y^b = x^{\mu-1}y^{q-1}$ with w -degree $m + 1$ has exactly $\mu q = d$ divisors. So $\mathcal{N}(\text{In}_{\prec}(I_D))$ is formed by these monomials.

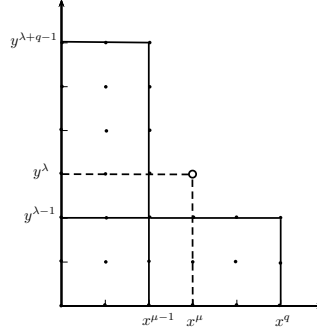


FIGURE 3. The number of monomials in $\mathcal{N}(\text{In}_{\prec}(\langle H, F \rangle))$.

Therefore x^{μ} is an element of $\text{In}_{\prec}(I_D)$. If $F \in I_D$ has leading monomial x^{μ} , by Proposition 2.9, I_D contains the ideal generated by H and F whose initial ideal is (x^{μ}, y^q) . So $I_D = (H, F)$ and the curve defined by F cuts D on \mathcal{H} . \square

Remark 4.2. Let C_m be the Hermitain code having distance $d = \mu q + \lambda(q + 1)$.

We obtain a divisor D corresponding to a minimum-weight codeword of C_m cutting \mathcal{H} with a curve \mathcal{X} unions of μ vertical lines and λ non-vertical lines that cut on \mathcal{H} an \mathbb{F}_{q^2} -divisor.

A more explicit description of how such lines can be chosen is given in the proof of Theorem 3.3. Here we only observe that the leading monomial of the polynomial defining such a curve \mathcal{X} is indeed $x^{\mu}y^{\lambda}$.

On the other hand, we point out that not all the polynomials F in $\mathbb{F}_{q^2}[x, y]$ with leading term $x^{\mu}y^{\lambda}$ correspond to minimum-weight codewords of the code C_m . The following results contains an explicit characterization of the “good” polynomials.

Corollary 4.3. *Let C_m be the Hermitain code having distance $d = \mu q + \lambda(q + 1)$. A polynomial F over \mathbb{F}_{q^2} with $\text{LM}_{\prec}(F) = x^{\mu}y^{\lambda}$ cuts over \mathcal{H} a divisor D corresponding to minimum-weight codewords if and only if the ideal $\langle H, F \rangle$ contains the field equations $x^{q^2} - x$ and $y^{q^2} - y$.*

Proof. In our hypotheses, D corresponds to minimum-weight codeword if and only if it is a \mathbb{F}_{q^2} -divisor on \mathcal{H} , namely if and only if it is contained in E . Clearly, this is equivalent to the condition on the corresponding ideals $I_D \supseteq I_E = \langle H, x^{q^2} - x, y^{q^2} - y \rangle$. \square

5. CONCLUSIONS AND FURTHER RESEARCH

The keystone to finding a geometrical characterization of any minimum weight codewords for the third and fourth phase was the choice of a different term order with respect to what can be usually found in literature, that is the **DegRevLex** with $y > x$.

The method developed in the present paper starting on this choice is proving to be powerful, and allows us to make progress in at least two distinct directions. There are evidences that complete intersections can provide a good descriptions of the minimum weight codewords also for the Hermitian codes C_m when $m < 2q^2 - 2q - 2$, and to codewords with a small weight.

On the other hand, our explicit description can be the suitable framework to develop computations on the weight distribution and estimate the value of PUE.

ACKNOWLEDGEMENTS

The second author was partially supported by the PRIN 2010-11 *Geometria delle varietà algebriche*, cofinanced by MIUR (Italy).

REFERENCES

1. E. Ballico and A. Ravagnani, *On the geometry of hermitian one-point codes*, Journal of Algebra **397** (2014), 499–514.
2. A. I. Barbero and C. Munuera, *The weight hierarchy of hermitian codes*, SIAM Journal on Discrete Mathematics **13** (2000), no. 1, 79–104.
3. A. Couvreur, *The dual minimum distance of arbitrary-dimensional algebraic-geometric codes*, Journal of Algebra **350** (2012), no. 1, 84–107.
4. C. Fontanari and C. Marcolla, *On the geometry of small weight codewords of dual algebraic geometric codes*, International Journal of Pure and Applied Mathematics **98** (2015), no. 3, 303–307.
5. P. Heijnen and R. Pellikaan, *Generalized hamming weights of q-ary reed-muller codes*, IEEE Trans. Inform. Theory, Citeseer, 1998.
6. J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Univ Pr, 2008.
7. T. Høholdt, J. H. van Lint, and R. Pellikaan, *Algebraic geometry of codes*, Handbook of coding theory, Vol. I, II (V. S. Pless and W.C. Huffman, eds.), North-Holland, 1998, pp. 871–961.
8. K. Lee and M. E. O’Sullivan, *List decoding of hermitian codes using gröbner bases*, Journal of Symbolic Computation **44** (2009), no. 12, 1662–1675.
9. K. Lee and M. E. O’Sullivan, *Algebraic soft-decision decoding of hermitian codes*, Information Theory, IEEE Transactions on **56** (2010), no. 6, 2587–2600.
10. C. Marcolla, *On structure and decoding of Hermitian codes*, Phd thesis, University of Trento, Department of Mathematics, 2013.
11. C. Marcolla, E. Orsini, and M. Sala, *Improved decoding of affine-variety codes*, Journal of Pure and Applied Algebra **216** (2012), no. 7, 1533–1565.

12. C. Marcolla, M. Pellegrini, and M. Sala, *On the small-weight codewords of some Hermitian codes*, Journal of Symbolic Computation (2016), no. 73, 27–45.
13. C. Munuera and D. Ramirez, *The second and third generalized hamming weights of hermitian codes*, Information Theory, IEEE Transactions on **45** (1999), no. 2, 709–712.
14. M. E. O’Sullivan, *Decoding of hermitian codes: the key equation and efficient error evaluation*, Information Theory, IEEE Transactions on **46** (2000), no. 2, 512–523.
15. M. Pellegrini, C. Marcolla, and M. Sala, *On the weights of affine-variety codes and some Hermitian codes*, Proc. of WCC 2011, Paris (2011), 273–282.
16. H. G. Ruck and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, Journal fur die Reine und Angewandte Mathematik **457** (1994), 185–188.
17. A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.
18. H. Stichtenoth, *A note on hermitian codes over $gf(q^2)$* , Information Theory, IEEE Transactions on **34** (1988), no. 5, 1345–1348.
19. H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.
20. K. Yang and P. V. Kumar, *On the true minimum distance of hermitian codes*, Coding theory and algebraic geometry, Springer, 1992, pp. 99–107.
21. K. Yang, P. V. Kumar, and H. Stichtenoth, *On the weight hierarchy of geometric goppa codes*, Information Theory, IEEE Transactions on **40** (1994), no. 3, 913–920.

Chiara Marcolla. DIPARTIMENTO DI MATEMATICA DELL’UNIVERSITÀ DI TORINO, VIA CARLO ALBERTO 10, 10123 TORINO, ITALY

E-mail address: chiara.marcolla@unito.it

Margherita Roggero. DIPARTIMENTO DI MATEMATICA DELL’UNIVERSITÀ DI TORINO, VIA CARLO ALBERTO 10, 10123 TORINO, ITALY

E-mail address: margherita.roggero@unito.it